UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,308	03/26/2004	Michael John Wray	B-5404 621794-8	7996

22879 7590 07/22/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
BAUM, RONALD	
ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
07/22/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/810,308	WRAY, MICHAEL JOHN	
	Examiner	Art Unit	
	RONALD BAUM	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,15 and 16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,15 and 16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the appeal brief filed on 05 May 2008, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139

2. Claims 1-13, 15 and 16 as presently amended/presented, are pending for examination. Claims 14 and 17 were previously canceled in the course of prosecution.

3. Claims 1-13, 15 and 16 are rejected.

4. Applicant's arguments with respect to claims 1-13, 15 and 16 have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible

harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985) (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969); and "ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claims 1-13, 15 and 16 are rejected on the grounds of a rejection based on nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 5, 5, 5, 5, 5, 5, 3, 5, 5, 5, 5, 6/7, 10 and 11 respectively, of U. S. Patent application 10/810,348 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

Although the conflicting claims are not identical, they are not patentably distinct from each other because [U. S. Patent application 10/810,348, e.g., claim 1] "A system comprising a trusted computing platform, one or more logically protected computing environments and ***a filesystem comprising a plurality of files and links defining access paths between said files*** ..." and [this instant application, e.g., claim 24] "A system comprising a trusted computing platform and one or more logically protected computing environments, each of which is associated with at least one service or process supported by said system ... *load* ***an operating system*** *into* ..." are related as genus/species insofar as the patent application species (i.e., U. S. Patent application 10/810,348) and application genus (i.e., this instant application), clearly are not patentably distinct. Further, the instant applications operating system aspects are broader in scope (i.e., genus) embodiments of the patent reference ' filesystem comprising a plurality of files and links defining access paths between said files ', elements (i.e., species), insofar as the phrases are used in the context of the claim limitations. More succinctly, the common inventive concept in both the instant patent application and associated reference patent application relating to the "*A system comprising a trusted computing platform, one or more logically protected computing environments* ..." and ***associated*** security policy aspects involved in the "logically protected computing environments..." secured operational (i.e., controlled/authorized access/processes)

characteristics, are such that the 'filesystem' aspects of the patent application reference is the more specific (i.e., species, *clearly constituting a* ***narrower interpretation***) case of the instant applications 'operating system' broader (i.e., genus), and is not made patently distinct by the dependent claim elements as claimed in the instant application.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-13, 15 and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Austel et al. ("Austel"), U.S. Patent No. 6,430,561.

8. As per claim 1; “A system comprising

a trusted computing platform and

one or more logically protected computing environments,

each of which is associated with

at least one service or process supported by said system,

the system being arranged to

load an operating system into

said trusted computing platform and

thereafter to

load onto said trusted computing platform

data defining a predetermined security policy

defining security attributes to be applied to

one or more of the at least one service or process

when said service or process is started

[ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments and a filesystem (i.e., an operating system), such that the integrity and security access class aspects (e.g., col. 6, lines 42-col. 7,line 25), and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

And further as per claim 15, this is the method embodiment claim for the system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

9. Claim 2 additionally recites the limitation that; "A system according to claim 1 wherein the policy included one or more security rules for
controlling operation of logically protected computing environments.".
The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, such that the integrity and security access class aspects (e.g., col. 6, lines 42-col. 7,line 25), and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

10. Claim 3 additionally recites the limitation that; "A system according to claim 2 wherein at least one of the one or more security rules is for at
least one of the logically protected environments and includes an execution control rule which defines the security attributes.".
The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file

system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

And further as per claim 16, this is the method embodiment claim for the system claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection.

11. Claim 4 additionally recites the limitation that; "A system according to claim 3, wherein said security attributes include or comprise one or
more capabilities to be provided to the respective logically protected computing environment when said service or process is started.".
The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

12. Claim 5 additionally recites the limitation that; "A system according to claim 3, wherein said security attributes include or comprise one or

more functions which change or modify the capabilities of the respective logically protected computing environment when said service or process is started.".

The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

13. Claim 6 additionally recites the limitation that; "A system according to claim 3, wherein when a service or process is started said security

attribute operates to cause the service or process to be placed and run in a specified logically protected computing environment.".

The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted

environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

14. Claim 7 additionally recites the limitation that; "A system according to claim 3, wherein said security attributes operate to modify a user id, a
group id or a logically protected computing environment in which a service or process is to be run.".

The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

15. Claim 8 additionally recites the limitation that; "A system according to claim 3, wherein said security attributes operate to change the root
directory of the service or process.".

The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

16. Claim 9 additionally recites the limitation that; "A system according to claim 5, wherein said execution control rule can raise or lower a
specified capability.".

The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

17. Claim 10 additionally recites the limitation that; "A system according to claim 5, wherein the security attributes operate to filter a set of
capabilities of a logically protected computing environment and modifying only one or more of said capabilities as selected by said filtering means.".
The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

18. Claim 11 additionally recites the limitation that; "A system according to claim 3, wherein said execution control rule specifies the service or
process to which it applies by identifying the associated logically protected computing environment, with the effect that said rule applies only to services or processes specifying that logically protected computing environment.".
The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing

platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

19. Claim 12 additionally recites the limitation that; "A system according to claim 3, wherein the files making up a service or process to which
said execution control rule applies are of read-only configuration.".
The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

20. Claim 13 additionally recites the limitation that; "A system according to claim 3, including means for monitoring operations performed by the
system which modify names of files making up services or programs to which said execution control rule applies.".

The teachings of Austel are directed towards such limitations (i.e., ABSTRACT, figures 1-9 and associated descriptions, whereas Austel discloses a system comprising a trusted computing platform, one or more logically protected computing environments, and ' an execute function … chaining … comprises starting another process running at potentially different secrecy and integrity access classes (e.g., col. 4,lines 53-col. 5,line 7)' such that the integrity/security access class aspects, and the processes/services associated with the classes as used in the trusted environments (i.e., the policy and associated security attributes insofar as related to the file system/run-time execution and access control), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

Conclusion

21. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid, can be reached at (571) 272-4063. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

/R. B./

Examiner, Art Unit 2139

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139